

Online Family Safety

Reboot Your Online Intelligence



AP Photo/Greg Baker

A director was stabbed and a young girl was raped. These are just 2 of the crimes that came with the use of social media. If you are worried about the online safety of the family, today is the best time to involve everyone and implement a cyber wellness program. The following are the initial steps that you can take.

- 1. Increase your online intelligence.** Educate yourself of the online risks and safety practices; the best place to start is Web Safety PH and Yahoo Safely. In a nutshell, here are some of the online risks that you have to address:
 - Online reputation damage resulting from untamed sharing on social networking sites. — Idiots don't need an enemy to destroy their online reputation.
 - Exposure to illicit and violent Internet content- exposure of kids to age inappropriate content
 - Cyber-bullying- use of social networks to bully or insult another person.
 - Online addiction- Addiction to computer games and social networking to the point that other daily responsibilities are neglected.
 - Malware — commonly known as virus that can be responsible for hacking, stealing of personal data and/or damage to data.
 - Identity theft- someone else will use your identity for personal gain or to destroy you.
 - Privacy issues — sharing too much personal information on the web, and improper configuration of a social networking account.

We will deal with each item in separate articles in future posts.

Another way to address above risks is to join a community that promotes cyber wellness and attend cyber wellness seminars that you can find.

SHAMELESS PLUGGING: My company, WSPH Training and Consultancy, offers a cyber wellness seminar dubbed "Watcha Webtrap!" The program has different variations to meet each group's need.

2. Increase the online intelligence of everyone in the family. Pass on to family members what you have learned. Create a summary of online safety practices and have it posted beside the family computer. If there is an opportunity, send them to cyber wellness seminars too.

3. Regulate access to the Web. Take on the role network admin and restrict access to sites that you deemed inappropriate, allow only games that are age appropriate and set time limit for kids. You can do this by using free tools like open dns, child safety features of your computer or use 3rd party application. We shall be discussing this too in future posts.

4. Set an example. The best way to promote cyber wellness to younger members of the family is to set an example. i.e, if kids are under 13, do not lie on their age just to create a Facebook account for them.

5. The computer should be located in a common area. It reduces online risks drastically.

6. Cyber wellness is everyone's responsibility. Adults share the responsibility of guiding the young. Online behavior is just a reflection of the real world, therefore good manners and right conduct still apply.

As parents of the digital age, it is our responsibility to make the internet a safer environment to our children.

Dealing With Online Addiction



AP Photo/Greg Baker

One of the risks kids face online is addiction, and parents should be equipped with basic knowledge to deal with it.

Online addiction is also called Web addiction or Internet addiction. It is the excessive computer use that interferes with daily life. Some sectors believe this is a new disorder, thus, also called in medical circles as Internet overuse, problematic computer use or pathological computer use or "Internet Addiction Disorder".

According to netaddiction.com, **if 5 of these eight symptoms are true**, then the person need serious routine alteration:

1. Do you or your kid feel preoccupied with the Internet (think about previous online activity or anticipate next online session)?
2. Do you or your kid feel the need to use the Internet with increasing amounts of time in order to achieve satisfaction?
3. Have you or your kid repeatedly made unsuccessful efforts to control, cut back, or stop Internet use?
4. Do you or your kid feel restless, moody, depressed, or irritable when attempting to cut down or stop Internet use?
5. Do you or your kid stay online longer than originally intended?
6. Have you or your kid jeopardized or risked the loss of significant relationship, job, educational or career opportunity because of the Internet?
7. Have you or your kid lied to family members, therapist, or others to conceal the extent of involvement with the Internet?
8. Do you or your kid use the Internet as a way of escaping from problems or of relieving a dysphoric mood (e.g., feelings of helplessness, guilt, anxiety, depression)?

There are physical symptoms too, of Internet addiction. According to Helpguide.org, web or computer addiction can also cause physical discomfort such as:

1. Pain and numbness in hands and wrists
2. Dry eyes or strained vision
3. Back aches and neck aches; severe headaches
4. Sleep disturbances
5. Pronounced weight gain or weight loss

Online addiction can be either due to online games, social networking sites, porn and chat services.

How to avoid online addiction

In some cases, Internet addiction is a symptom of a family problem. It becomes an outlet for kids to escape problems in the family. For example, in online games, players can banish their enemies with a snap of a finger or with a single breath of fire. The "enemies" may represent the family problems they wish they could banish.

The family should view online gaming as tool for bonding and to unwind. This should never be use as a high-tech nanny to keep the children behaved. If kids began to live around gaming, then other areas of development will be neglected.

On general terms, online addiction can be avoided by the following:

1. Limit their time on the web.

2. Enhance real life relationships; virtual relationships cannot replace real ones.
3. Do things together with your kids, household chores, washing cars, doing their homework or school project.
4. Sponsor a social gathering in the house and invite your kids friends and cousins.
5. Promote a balance life by encouraging them to be involve in various school and community based activities.

If the symptoms we discussed persist, it is only proper to seek professional help.

Dealing With Social Networking Sites



AP Photo

Social networking sites are supposedly a fun place. But the innocence of our kids and our own ignorance can bring harm to the family. Follow these safety practices and teach the same to kids, and your family can avoid the common pitfalls.

- 1. Define you individual online philosophy.** - This will govern your online behavior (i.e., if philosophy is for family use, one can share liberally but restrict connection to family members only). If philosophy is for networking, one can add anyone but sharing is conservative.
- 2. If you can, share as less personally identifiable information.** - Free services thrive on the information you give out. Where there is data and info, money flows.
- 3. Do not disclose family members.** - Your real life friends know them, cyber criminals don't.
- 4. Encourage kids to use avatars instead of pictures in their profile, and an alias in their handle.** - This will help protect their privacy.
- 5. After opening an account, alter the default privacy settings.** - Choose only the info that you wish to share to a specific group of people.

6. Do not share real time picture of family. — My son knows that he should not share real time pictures and that he should un-tag himself if his friends tag him in Facebook photos. If and when I will share a family pic for public access, I share those that were taken 10 years ago or older.

7. Observe age restriction and other requirements spelled out in terms of use/ end user license agreement. — There are built-in safety reasons that go with these, i.e. access to games, exposure to marketing ads.

8. Do not disclose "real time" location. - If using location services, only check-in when you are about to leave the place, or when you are giving a generic location.

9. Connect with your kids online. — It's better if parents have access to the account of kids. This is unpopular, but if parents are responsible stewards and will be a happy lurker, kids may be convinced to share password.

10. Teach kids to follow these additional safety measures.

A. Do not engage a stranger in a text or video chat.

B. Do not add a stranger in his/her friends list.

C. Do not meet a stranger offline.

D. In case of a community eyeball, only participate if the event will be held in a public place and will be accompanied by an adult.

E. Discuss with you, as parent, uncomfortable experiences on social web. Your kid can use built-in features of a social networking site, like Facebook, to do this.

Dealing With Online Games



AP Photo

Games are always a hit among kids—be they old-fashioned or hi-tech ones. But combining games with technology spawned a new challenge for parents.

As a modern generation parent it is but proper to be involved with our kids [online] gaming activities to ensure balance on kids growth.

Here are some practical tips for parents:

1. Know the games your kids play. As a parent you should know what the contents of the games are. This way, you are in better position to guide and mentor your kids. Giving a "blanket" approval or restriction to gaming is also not healthy.

2. Allow only age-appropriate games. Games should be age appropriate to your child, it prevents early exposure to materials that can influence behavior.

3. Regulate play time and restrict access to if needed. Managing the time consumption of your kid's access to games can anticipate potential addiction and it can develop your child's disciplined trait.

4. Play the games with your child. It will not only help you bond with your kids, but you will be in better position to do item No. 5.

5. Talk about what you see. If your child discovers material that he/she finds disturbing or that you find inappropriate, talk about it. This is a great opportunity to let your child know what your values are as well as to help him/her deal with images that may be troubling.

6. Make it public. You can't monitor what you do not see, you can't manage what you do not know

7. Give feedback. If you find inappropriate contents on the game, or the school grades are being affected, feel free to touch base with the gaming companies. Some gaming companies work with parents in restricting log-in access to the kid's account. If your kids are using Internet café's to play games, talking with the Internet café operator or the *barangay* chair may help.

Teaching Kids to Value Privacy



AP Photo/Katsumi Kasahara

The Philippines, which has been dubbed as the "social networking capital of the world," has the highest social media penetration rate with more than 26 million online users.

According to SocialBakers.com, 20 percent of Facebook users are 13 to 17 years old. These roughly means five million kids need to be guided so that sensitive personal and family information will not be divulged to everyone.

Below are important things parents should teach their kids:

- Provide minor information. Give out only basic or general information that are common knowledge. Avoid participating and allowing polls or survey, application and sites that are suspicious.
- Never ever share home address and phone numbers.
- Do not disclose parents and siblings. Real friends know who they are.
- Use avatar as profile picture, or use old pictures.
- Don't respond to unknown sender of messages that they receive. Delete or remove them away quickly.
- Do not click links that can be found on their Facebook wall or inbox.
- Do not disclose real time locations.
- Accept only people they know, so your profile access will be limited to those people who you really know.
- Empty web browser cookies or history, when using public computers to avoid unauthorized access to their profile or account.
- Think about personal and family security before sharing or publishing post of status, shout out, pictures in social networking sites.

Likewise, parents should do the following with their kids:

- Read and explain the terms of service, rules and most importantly the privacy policy.
- Customize the privacy setting, in selecting information that parents think are reasonably adequate to be displayed on kid's profile.
- Create a strong password; enter hard to guess password or unusual passwords. Create and set up alternative e-mail address that can connect to the account.

Applying the tips above can minimize intrusion to personal and family privacy.

Ref.: <http://ph.news.yahoo.com/blogs/safetynet/online-family-safety-reboot-online-intelligence-041132930.html>

Remark it's ALL 5 pages gathered here ☺

Look MUCH more here: www.InternetAbuse.AboutPhilippines.ph and www.WebSafety.PhilippineChildren.ph